UKERNA

JANET Roaming Service (JRS)

USER GUIDE

Contents

Summary 3
1 Introduction 4
1.1 What the JANET Roaming Service Can Offer You 5
2 End User Information 6
2.1 Roaming AUP 6
2.2 Preparing to Connect to the JANET Roaming Service 6
2.3 Your Roaming Credentials 8
2.4 How to Locate JRS Guest Network Services 9
2.5 Connecting Securely at the Visited Site 10
2.6 How to Get Support 13
2.7 How to Report a Security Incident 13
3 Glossary 15
4 Site-Specific JRS Information and Visitor Checklist 17
Appendix 1 – Technical Details of User Services 18
Appendix 2 – 802.1X Supplicant Configuration 19
Appendix 3 – Configuring Dynamic IP Address Allocation 21

Summary

The JANET Roaming Service (JRS) is an initiative designed to provide roaming network access between participant sites in the UK education and research sectors for staff and students. JRS is a member of the international eduroam federation, which extends this facility world-wide.

This guide sets out information required for a visitor to a JRS-enabled site to make use of their guest network(s), both in terms of the preparations they need to make before their visit and actions required when on site. It also describes the service policies and responsibilities incumbent upon a JRS user.

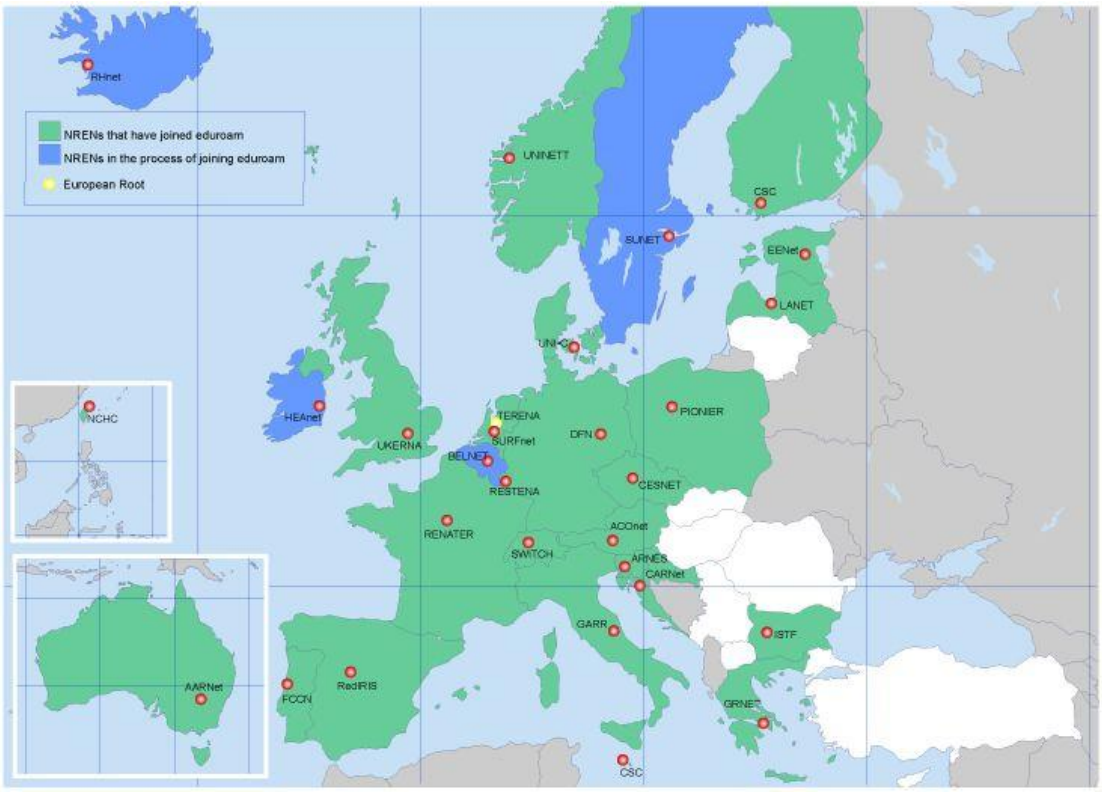
A digest version of this guide which concentrates simply on how to connect via JRS is also available.

1 Introduction

The **JANET Roaming Service** (JRS) was developed to enable users from any participant site in the UK to use guest networking services at any other participant site to access the Internet or external services provided by their home site. For example, JRS can let you use the network for tasks such as e-mail access and web browsing when away from your home organisation without having to make prior arrangements for a guest account, carrying proof of identity, or paying for commercial services. Instead, your familiar 'home' credentials authenticate you to educational network services both across the country and internationally.

JRS in the UK has joined forces with similar initiatives world-wide to form the **eduroam federation**. Users from UK participant sites can gain network services in many countries throughout mainland Europe and beyond. Current membership of the eduroam federation can found at:
http://www.eduroam.org/

The eduroam federation



Eduroam participant sites display a distinctive eduroam logo (developed and trademarked by TERENA) to ensure that roaming services can be easily recognised. The JRS logo incorporates the eduroam symbol to indicate membership.

1.1 What the JANET Roaming Service Can Offer You

Sites that participate in the JRS system in the UK (or the eduroam federation overseas) may elect to make some form of guest network access available to visitors to their campus. Precisely what any particular site offers in terms of networking services to its visitors is determined by their local technological and policy constraints, but there is a minimum set of services specified by JRS in the UK (in line with wider federation guidelines) that all such visitor services must make available. These are:

- Web browsing, including secure websites
- E-mail, send and receive
- VPNs (Virtual Private Networks)
- File transfer
- Remote Shell and Desktop

See Appendix 1 for a detailed listing of the protocols and ports involved.

This minimum range of services covers the vast majority of user activity, and ensures a rich networking environment for guests that will facilitate their work away from their home site. However, some of these services may be provided through filters that differ from those of your home site. For example, if you rely on your home site to provide virus filtering or firewalling, be aware that these provisions may not protect you at the visited site. Similarly, if the visited site's AUP (Acceptable Use Policy) differs from that of your home site then you may not be able to access some web sites or other network resources that you would expect to from your home site (either through being forbidden to do so by the local AUP or by such content being actively blocked). The central JRS web repository maintains a list of links to specific organisations' JRS pages which detail these local policies.

Note, however, that for you to use any services hosted at your home site via a JRS-enabled visitor network, they must be accessible to off-site users – i.e. your home site's firewall must allow external access to them. Put another way, JRS guarantees that your traffic related to these services will be allowed *out* of the visited site, but your home site controls whether it can get *in* to your home systems. So, for example, if your home site does not offer remote access to e-mail then JRS cannot be used to gain access to it. It is also possible that some user services may be provided through a different medium to users when offsite: for example e-mail access may be offered via a web interface for remote access rather than the more usual mail client software used when at the home organisation. In most cases, VPN services are the solution to this problem. If you are not sure whether a given service will be accessible or in what form, check with your home IT support services.

All JRS sites in the UK are required to publicise the services they offer, and any related local policies for acceptable use, so look for signage or web-based information before you connect.

2 End User Information

2.1 Roaming AUP

Your home organisation will enforce a local AUP for network services which you should already be aware of, and which will incorporate additional national rules such as the JANET AUP. As a condition of UK JRS membership, your organisation extends this policy to cover your network activities when you are off-campus and connecting to a visitor facility via JRS (or, internationally, via eduroam). This means that when you use network facilities while visiting a site you must not break any of the rules that normally apply when you are on-site at your home organisation. A home organisation can apply disciplinary measures for any breach of their computing regulations (no matter where the user is physically located at the time of the infringement) when credentials it has issued are being used to gain network access.

As well as continuing to be governed by your home regulations, it is your responsibility as a JRS visitor to check the local rules and respect them as well. The site you are visiting is obliged to publish its local policy. Although most academic organisations apply similar policies, the possibility of difference does exist: in this event, the more restrictive of the policies applies.

So, as a JRS user you must:

a) **Be aware of your home site AUP** and understand that it applies equally when you are visiting another JRS-enabled site.

b) Undertake to **read the overall JANET Roaming Service policy document** before using the service, at:

   http://www.ja.net/documents/services/janet-roaming/policy.pdf

c) Undertake to **read the visited site's AUP** before you start to use their network, and to abide by it.

d) **Stop immediately** if you are told that you are breaking any of these policies.

In all cases, if you are unsure whether a given networking activity is permitted by your home or local policies in force, you should seek clarification from IT staff in the appropriate location before proceeding.

2.2 Preparing to Connect to the JANET Roaming Service

Guest services at JRS-participant sites in the UK (where provided) may vary in scope, available technology and purpose within the organisation concerned. To accommodate this, JRS defines three differing specifications, referred to as 'tiers' of service, which sites may adopt. Any given site may offer visitor network services within more than one tier, for example to accommodate visitors with client devices (PDAs, laptops etc.) of differing capabilities.

As a user, you must determine which tier(s) are on offer at any site you visit, by consulting the home site's JRS web pages, on-site signage, or speaking to IT support staff. The way in which you connect to the guest network will be determined by the characteristics of the particular tier(s) they offer and/or you select (see 2.5 below).

> *You should connect to the highest-numbered tier available that your client device can support, as this will provide the greatest security and range of functions to you.*

At present, **tier JRS3** represents the most advanced roaming service available, but may only be available for a limited range of client devices. By contrast the lowest, **tier JRS1**, is universally accessible since it requires only a web browser but offers a less secure networking environment than the higher tiers (although still offering a safe medium for most network tasks if the precautions noted below are observed). **Tier JRS2** represents a compromise between these extremes and will be the most commonly encountered implementation of a JRS-enabled visitor network.

Tier	Client requirements	Security level
JRS1	SSL-aware web browser with 'well-known' root certificates installed.	Low (additional precautions recommended to use securely)
JRS2	802.1X supplicant. WEP support as a minimum for wireless access.	Medium
JRS3	802.1X supplicant. WPA2 support for wireless access.	High

2.2.1 Before you set out

There are a number of preparatory steps you must take when planning a visit to a JRS site which will make the connection process simpler.

1) **Ensure you know your JRS credentials, including your realm** (see 2.3 below).

2) **If your home site has an 802.1X-based JRS visitor service (i.e. tier JRS2 or higher) then configure your device to use the <u>home</u> service before you leave**. You may well have to liaise with your local IT support staff to get everything working before you set out. The UK roaming service has been designed such that if you can connect to a JRS2 or JRS3 tier successfully at your home site, you can connect to that same tier of service at any other JRS site *without changing your configuration in any way.*

3) **Obtain the contact details for your home site JRS support service**. Even though you are physically off-site, your principle avenue of obtaining support is still your <u>home</u> organisation, so you will need to know the relevant

telephone contact numbers, web page addresses etc. to get help in case you have any difficulty. See section 2.6 below.

4) **Check the AUP of the site you are visiting** via the web, either at their own JRS webpage(s), or via the central repository of JRS information:
http://www.ja.net/roaming

   If travelling overseas, you should check local policies linked via:
http://www.eduroam.org

5) **Confirm that all network services you will need to use remotely are permitted** by their regulations. If not, you may need to make special arrangements with your hosts there. Remember the common set of protocols offered by all JRS sites, as detailed in the appendix.

6) **Ensure that your device is prepared to accept dynamically-assigned IP addresses.** Your home site may already use automatically-assigned network addresses, but if it does not, you should make sure both that you have the administrative rights on your device to enable assigned addresses and that you know how to do so. Your home site IT support staff will assist with these settings if required.

2.3 Your Roaming Credentials

The username and password that you use at your **home site** form the basis of your **roaming credentials**. However, JRS needs to know where you are from as well as who you are in order to authenticate you, because it refers your access request back from the **visited site** where you are trying to log in to your original home site for authentication. To achieve this, you will be informed of a JRS **realm** by your home IT staff, which you need to attach to your username when you use it in a roaming context. So, your *username* at the home site becomes *username@realm* when you log into a visited site via JRS – the password stays the same in both cases. The realm you are provided with will typically consist of a short sequence identifying the location, a portion identifying that site as an academic organisation, and a country code, all separated by periods ('.'s).

For example, consider the user Joe Bloggs from Example University. His home username is '*jbloggs*'. His local IT support tells him that the JRS realm that applies to him is '*example.ac.uk*'. His JRS username is therefore '*jbloggs@example.ac.uk*'. If he types this and his usual password into any JRS-enabled authentication system, they will be checked with his home organisation and, on successful authentication, will allow him to access the services provided by the visited site.

Notice that while a JRS username looks like an e-mail address, since it is doing the same job (identifying who you are and where you come from), it is not necessarily the same as your actual e-mail address. It is important not to confuse the two by attempting to log into a JRS-enabled network with your e-mail address (either your home organisation one or even a third party one such as for Hotmail) since it will not work. You also should not try to guess what your realm might be: due to a number of organisations having similar

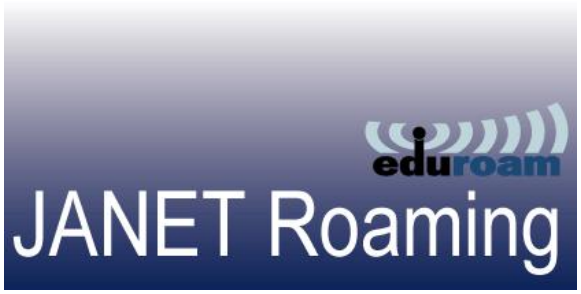
names, this might result in your credentials being checked in the wrong place and failing to work.

2.4 How to Locate JRS Guest Network Services

In the UK, a central register of JRS participant sites is maintained at:
http://www.ja.net/roaming

Similar national registers are maintained by other member nations of the eduroam federation, and can be reached from the federation website:
http://www.eduroam.org

Individual JRS-participant sites in the UK undertake to advertise their JRS-enabled services clearly to visitors. For wireless services, JRS adopts the standard 'eduroam' broadcast SSID (ensuring compatibility for visitors from non-UK eduroam federation member organisations) but this will in most cases be supplemented with signage in the locations where such services are available, displaying the JRS logo. *You may also encounter the SSID 'eduroam-web' used to advertise a tier JRS1 web-redirect service, or the SSID 'eduroam-wep' used to advertise an implementation of tier JRS2 (see 2.5.1 below and elsewhere).*



The sign displayed at JRS-enabled sites

At some sites, specific Ethernet ports may be made available for wired connection to JRS-enabled guest services, and these too will be clearly indicated by signage. If in doubt, seek advice from your host or the visited site IT support staff.

You should not connect to a wireless service or plug into a wired network in the hope of finding a JRS-enabled facility without some clear indication beforehand that it is indeed intended as a guest service.

It is an unfortunate fact of life that in using the Internet, care must be taken over whom to trust with sensitive information such as passwords. Your user credentials not only give access to personal information, they might also form the first step in attempts to steal computing resources or break into central systems at your home site. It is vital, therefore, that you take steps to ensure that you are associating with a legitimate, official JRS visitor network before trying to log in to it. This issue arises with tier JRS1 web-redirected services (see below for a discussion of tiers), where you are prompted to enter your credentials into a web form. Since all of the design and imagery of such pages can readily be duplicated to create a 'rogue' system, you must pay particular attention to ensuring that the page is offered over a secure link (e.g. look for a padlock icon in Internet Explorer), and to any dialogues arising relating to

mismatches in the security settings of the website certificates. You should follow any guidelines specified by your home site in identifying legitimate services, and if in any doubt check with authorised staff at the visited site.

JRS, the UK implementation of eduroam, is designed to use the 802.1X protocol in tiers JRS2 and JRS3, which guards against this kind of identity theft. Your credentials are protected right up until they arrive at your home organisation for authentication.

2.5 Connecting Securely at the Visited Site

The connection procedure differs slightly depending upon which tier of JRS service is being offered and which you choose to connect to.

2.5.1 Connection Requirements Common to All Tiers

Whichever tier you use, accessing JRS services over wireless networks requires you to associate with a service advertised via a broadcast SSID. You should therefore ensure that you are familiar with how to do this before you try to use a JRS service at another site.

At any site, the SSID ‘eduroam’ is assigned to the most secure implementation of the roaming service available (i.e. the highest numbered JRS tier). This ensures that a visitor with a client device that is configured to associate with the ‘eduroam’ SSID is always presented with the most secure available guest network service by the visited site, and also ensures compatibility for visitors from overseas participants in the eduroam federation. Should a visitor desire to connect to a lower JRS tier for any reason (such as limitations of their client device), an alternative SSID carrying the ‘eduroam-’ prefix will be available. This is discussed in more detail below under each tier’s heading.

JRS services (both wireless and wired) will also supply your device with a local IP address for the duration of your session. You will therefore need to configure your computer to accept an automatically assigned address. This process varies according to operating system. (See Appendix 3 below for instructions covering Windows XP.)

2.5.2 Tier JRS1 – Web Redirection Authentication / No Encryption

Tier JRS1 services represent a legacy technology option for sites in the process of upgrading to the higher (and more secure) JRS tiers. As such, they provide less in the way of data security for the user and should ideally be used only with protocols that apply their own encryption schemes. It is expected that tier JRS1 services will be withdrawn once the technologies required for higher tiers are widely available.

> Where a visited site offers only tier JRS1, it will be advertised via the broadcast SSID ‘**eduroam**’. (Note that tier JRS1 may also be offered on a wired network.)
>
> Where a visited site offers higher tiers alongside JRS1, the SSID ‘eduroam’ is assigned to the most secure available service (i.e. the highest numbered tier available), and tier JRS1 will be advertised via the broadcast SSID ‘**eduroam-web**’.

Having associated with the network, whether by connecting to the wireless network identified by the appropriate SSID or by connecting to an identified visitor service port on a wired network, you should first launch a web browser. Whatever your homepage is set to, the network will intercept the web request and redirect you into the web-based authentication process for the service.

At this point, the authentication mechanism will check whether your browser recognises the security certificate offered by the service. **If it does not, or the certificate is out of date or any other problems with it are indicated, you must not proceed, even though you will be offered the opportunity to trust the malformed certificate the website offers. Official JRS visitor networks will always offer a valid certificate.** Where there are problems with the certificate it *may* indicate that you have been intercepted by a 'rogue' website designed to trick you into giving away your credentials (see 2.4 above). Report all certificate problems to IT staff at the visited site.

Following a successful certificate check, you will be presented with the JRS1 Login Screen. The web interface for tier JRS1 is developed from a common web interface template at all JRS sites offering this tier.

You should **confirm that the login dialogue is presented on a secure webpage** (i.e. via HTTPS) before entering your JRS credentials. In Internet Explorer, this is indicated by a closed padlock symbol in the information bar at the bottom of the window. Other operating systems use different mechanisms to indicate a secure link – consult your relevant documentation.

You should also check any notices, local policies or regulations linked from the login pages before proceeding.

Following a successful authentication, you will then be granted a period of network access, at least to the services detailed in 1.1 above. The length of this access period and any mechanisms provided for actively logging off of the network when finished will be detailed in the visited site's JRS documentation.

2.5.3 Tier JRS2 – 802.1X Authentication / '802.11'-based Encryption

Tier JRS2 offers both secure authentication and a (variable) measure of data encryption to maintain your data privacy during your session.

As a guideline, tier JRS2 services offer a level of data protection sufficient to deter 'real time' exploits such as hijacking your session or inserting bogus data into your communications. However, given sufficient time and computing power, a *recording* of your network traffic on a tier JRS2 service could be deciphered, so as with tier JRS1 it is recommended that you should **only use protocols that apply their own data-security mechanisms (such as SSH, VPN or HTTPS websites, for example) over a tier JRS2 service when dealing with sensitive or private data. Otherwise, make the assumption that someone could potentially read your data later, and act accordingly**. Tier JRS2 is the current 'target' level for visitor services that all sites are working towards, until hardware support for tier JRS3 becomes more widely available.

Where tier JRS2 is the highest-security implementation of JRS available, it will be advertised by the broadcast SSID of '**eduroam**'.

Where tier JRS2 is available in parallel with tier JRS3, it will be advertised by the broadcast SSID of '**eduroam-wep**'.

The definition of tier JRS2 leaves a certain amount of freedom for the visited site to determine what degree of data encryption they apply after you authenticate. In order of security the standards which may be deployed are WEP, WPA and WPA2. Typically, a JRS2 implementation will offer a degree of backwards compatibility – for example, a JRS2 service that supports WPA connections will also support WEP connections. The local roaming service documentation will indicate what options are available and what benefits they offer.

- *If your home site already deploys a JRS tier using 802.1X Authentication.* All JRS visitor services in tier JRS2 and tier JRS3 should be completely transparent to users whose device is already appropriately configured to use their home JRS/802.1X wireless service with JRS credentials. No reconfiguration will be required. Since the login process is determined by the supplicant software you run on your client device communicating back to your home site (whether or not this traffic crosses a visited network in between), the processes involved and the login dialogues you see will always be the same. In fact, if you see any differences in the process, you should stop immediately as it is possible you are not connected to an official trusted JRS2 service. Your home site will provide full instructions on how to connect to their local service.

- *If your home site does NOT use 802.1X Authentication*, i.e. your home site only offers a tier JRS1 service, or does not offer any visitor network facilities, or if the supplicant software is not currently set up on your laptop or other device, you will need to configure PEAP-based 802.1X manually. Detailed instructions on this process for the Windows XP SP2 native supplicant are presented in Appendix 2 of this document.

- Other supplicant software for 802.1X connection does exist for Windows, both commercial and open source. If your home site makes use of a particular supplicant by preference, use that in accordance with the instructions provided by your home IT support.

2.5.4 Tier JRS3 – 802.1X Authentication / WPA2 Encryption

Tier JRS3 services offer strong encryption, sufficient to deter all but the most determined attempts to break security. Therefore, **tier JRS3 services are considered safe for the transfer of sensitive information** such as user credentials without further encryption. Additional precautions are always advisable, however, as data may subsequently traverse public networks.

At present, tier JRS3 is a special 'advanced' level of service providing the highest security available. It will therefore be available at only a limited number of JRS

participant sites. Tier JRS3, when available, is always advertised via the broadcast SSID of '**eduroam**'.

Connection procedures to a JRS3 service will be exactly as per tier JRS2 (see 2.5.3 above).

2.6 How to Get Support

Your home site is your primary point of support, wherever you may be physically located. This is because JRS is designed such that all the actual processing of your authentication occurs at your home site, and so support staff at the visited site have limited access to information that may help them troubleshoot any difficulty you are having.

Arrangements will vary by organisation, but typically you will have access to a telephone number for JRS support at your home site, supplemented by configuration information on the web. That said, support staff at the visited site are the appropriate contacts for certain kinds of information, such as where access points are located, how to find the local AUP, etc. It is also possible that in resolving an issue, your home site may contact staff at the visited site to co-ordinate with them in addressing a problem.

> *When using eduroam facilities overseas, bear in mind the normal support hours at your home site!*

JRS in the UK does have a centralised support team, but they liaise directly with designated IT staff at the participant organisations. Users should never attempt to raise an issue directly with the central team.

2.7 How to Report a Security Incident

As a user of JRS, you assume responsibility for all activities undertaken with the authority of your personal JRS credentials. If your credentials are used to break the law or any organisational policy then you will be presumed to be responsible. It is therefore essential that you maintain the privacy of those credentials. You should never reveal them to anyone else, or leave them written down where someone else might read them.

> *Note that there is no legitimate reason for the IT staff at the visited site to request your JRS password, although they may need your JRS username or realm in order to check logs if you are having a problem.*

The JRS system is designed to keep your credentials private as it passes them across the network from the visited site back to the home site to be authenticated. All visited sites undertake to maintain secure services for this purpose, and are required to notify your home site and JANET-CERT (the security team for UK education and research sectors) if the security of the system may have been breached, either by a security incident or by your behaviour as a user. Visited sites, the national JRS core and your home site maintain logs of all use of the JRS system for the tracing of such incidents.

As a user, you must:

- Keep your credentials private!

- Take steps, as instructed by your home site when they train you on JRS usage, to confirm that the JRS-enabled visitor services into which you type your credentials at a visited site are indeed legitimate, rather than rogue systems created by inimical third parties to trick you into providing your password.

- Only use network services that provide an appropriate level of security for your credentials and personal data.

- Avoid using any network service in a way that could be construed as an attempt to determine someone else's credentials, interfere with their sessions in any way or deny overall access to the service. The latter category might include broadcast of wireless beacons, advertising routing information, or replying to DHCP broadcasts.

- Co-operate with any instructions by authorised staff at the visited site relating to secure use of their guest network(s).

Should you suspect that the privacy of your credentials has been breached, or that someone has tried to induce you to reveal your credentials, you should inform the IT support contact advertised on the visited site's JRS documentation of your concerns. They will then escalate the issue appropriately.

3 Glossary

In the course of development, the JRS has developed specific terms for the various roles in its infrastructure. The technologies deployed also carry their own technical jargon. This glossary is designed to help clarify some of the language that is used in describing the service.

AUP	Acceptable Use Policy – the set of rules governing what a user may or may not do whilst connected to a network.
CA	Certificate Authority – the trusted source that provides certificates to a group of associates. The eduroam central support team acts as the CA for all eduroam tier 1 services.
CERT	Computer Emergency Response Team – those responsible for reacting to computing security incidents. The UK academic team is JANET-CERT.
Certificate	In this context, a data file obtained from a trusted source that allows a user to confirm that a given network service (such as a web page) is also validated by that trusted source.
Eduroam	The name of a federation of roaming network access initiatives in the educational sphere, of which the JANET Roaming Service programme in the UK is a member. Users with a JRS home site in the UK can gain guest access to networks at any eduroam organisation, worldwide.
Home site	The organisation that issues you with your username and password, i.e. where you are registered as a member of staff or student.
JANET	The data network that connects the UK's education and research organisations to each other, as well as to the rest of the world through links to the global Internet.
JRS	The JANET Roaming Service
JRS credentials	Your username and password for requesting access to JRS-enabled networks. Usually based on your **home site** credentials, but with the addition of the appropriate **realm** to your username. E.g. user@realm, janedoe@example.ac.uk
Realm	A sequence of characters that identifies a home site, and is added to a home username to create an eduroam username.
Root certificate	A single certificate that the user can install to check the identity of a large number of network services. For example, the single eduroam root certificate allows the validation of all UK eduroam tier 1 services.
SSID	The 'name' of a wireless network that allows you to pick it from a list of those your client device can detect.
Tier	A level of service within the overall JRS programme in the UK. Multiple tiers are implemented in order to accommodate the various levels of expertise and resources at the wide variety of JRS participant sites, and to give an upgrade path as the technologies involved develop and mature. As a rule of thumb, a higher-numbered tier represents a more secure networking environment.

UKERNA	United Kingdom Education and Research Networking Association – the company responsible for the operation and development of JANET.
Visited site	The organisation you are visiting when you request network access via JRS, i.e. your physical location.

4 Site-Specific JRS Information and Visitor Checklist

If you obtained this document directly from UKERNA, please consult your local IT Support and the JRS website of the organisation you intend to visit in order to fill in the blanks. Organisations distributing this document to their users may wish to edit this page to include their site-specific information.

Don't write down your password here!

a) About my home site

My realm is:	
My home JRS support website address is:	
I have read my home JRS AUP, and it is available at address:	
My home support telephone number is:	

b) Pre-visit checklist

My device works with my home site JRS service (where present) and is prepared to accept dynamically-assigned IP addresses. [ ]

I have read the AUP of the site I am visiting. [ ]

I have confirmed that the network facilities I require are provided by the guest service at the site I am visiting. [ ]

I have confirmed that my home site permits remote access to the facilities I require from the visited site. [ ]

Appendix 1 – Technical Details of User Services

JRS guest network services will *as a minimum* offer the following access to services.

1) **E-mail**
   - **a.** IMSP: TCP/406 egress and established.
   - **b.** IMAP4: TCP/143 egress and established.
   - **c.** IMAP3: TCP/220 egress and established.
   - **d.** IMAPS: TCP/993 egress and established.
   - **e.** POP: TCP/110 egress and established.
   - **f.** POP3S: TCP/995 egress and established.
   - **g.** SMTPS: TCP/465 egress and established.
   - **h.** Message submission: TCP/587 egress and established.

2) **Web**
   - **a.** HTTP: TCP/80 egress and established.
   - **b.** HTTPS: TCP/443 egress and established.

3) **VPN**
   - **a.** Standard IPSec VPN: IP protocols 50 (ESP) and 51 (AH) both egress and ingress; TCP/500 (IKE) egress only.
   - **b.** IPSec NAT traversal: UDP/4500 egress and established.
   - **c.** Cisco IPSec NAT traversal: TCP/10000 egress and established.
   - **d.** PPTP: IP protocol 47 (GRE) egress and established; TCP/1723 egress and established.
   - **e.** OpenVPN: TCP/5000 egress and established.
   - **f.** IPv6 Tunnel Broker NAT traversal: UDP/3653 and TCP/3653 egress and established.

4) **Remote Desktop**
   - **a.** RDP: TCP/3389 egress and established.
   - **b.** VNC: TCP/5900 egress and established.
   - **c.** Citrix: TCP/1494 egress and established.

5) **Directory Services**
   - **a.** LDAP: TCP/389 egress and established.
   - **b.** LDAPS: TCP/636 egress and established.

6) **Secure Shell**
   - **a.** SSH: TCP/22 egress and established.

7) **File transfer**
   - **a.** Passive (S)FTP: TCP/21 egress and established.

UKERNA:
UKERNA manages the networking programme on behalf of the higher and further education and research community in the United Kingdom. JANET, the United Kingdom's education and research network, is funded by the Joint Information Systems Committee (JISC).

Contact:
JANET Customer Service
UKERNA
Atlas Centre, Chilton, Didcot
Oxfordshire, OX11 0QS
Tel: 0870 850 2212
Fax: 0870 850 2213
E-mail: service@janet.ac.uk

Copyright:
This document is copyright The JNT Association trading as UKERNA. Parts of it, as appropriate, may be freely copied and incorporated unaltered into another document unless produced for commercial gain, subject to the source being appropriately acknowledged and the copyright preserved. The reproduction of logos without permission is expressly forbidden. Permission should be sought from JANET Customer Service.

Trademarks:
JANET®, SuperJANET® and UKERNA® are registered trademarks of the Higher Education Funding Councils for England, Scotland and Wales. The JNT Association is the registered user of these trademarks.

Disclaimer:
The information contained herein is believed to be correct at the time of issue, but no liability can be accepted for any inaccuracies. The reader is reminded that changes may have taken place since issue, particularly in rapidly changing areas such as internet addressing, and consequently URLs and e-mail addresses should be used with caution. The JNT Association cannot accept any responsibility for any loss or damage resulting from the use of the material contained herein.

Availability:
Further copies of this document may be obtained from JANET Customer Service at the address above. The document is also available electronically from:
http://www.ja.net/services/publications/

© The JNT Association 2006